WE CLAIM:

1. A pseudorandom number generating apparatus wherein said pseudorandom number generating apparatus comprises:

a state storage section;

a buffer;

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation;

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock; and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs; and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

10051567.011502

2. A pseudorandom number generating apparatus

according to claim 1, wherein

said state transformation section comprises a first operation section and a second operation section,

said first operation section comprises: an input section for accepting 1st and 2nd blocks included in three blocks stored in said state storage section, and a block stored in the buffer, as inputs thereof; a first nonlinear transformation section for conducting nonlinear transformation on said 1st block and said block stored in the buffer and outputting n-bit data; a third operation section for receiving an output of said first nonlinear transformation section and said 2nd block as inputs thereof and conducting a logical operation on the inputs; and an output section for outputting said 1st block and a result of the operation conducted by said third operation section, and

said second operation section comprises: an input section for accepting either output of said first operation section, a 3rd block stored in said state storage section, and said block stored in the buffer, as inputs thereof; a second nonlinear transformation section for conducting nonlinear transformation on either output of said first operation section and said block stored in the buffer and outputting n-bit data; a fourth operation section for receiving an output of said second nonlinear transformation section and said 3rd block as inputs thereof and conducting a logical operation on the inputs; and an output section for

10046157.041502

outputting either output of said first operation section and a result of the operation conducted by said fourth operation section.

3. A pseudorandom number generating apparatus according to claim 2, wherein

said state transformation section further comprises a permutation section, and

said permutation section conducts permutation so that operation results of said third and fourth operation sections will be stored in said state storage section as blocks different from blocks respectively input to said third and fourth operation sections.

10025457 .031502

4. A pseudorandom number generating apparatus according to claim 1, wherein

said state transformation section conducts the following processing:

$x_L \leftarrow a_H;$

$x_H \leftarrow a_M \text{ XOR } F(a_H, b_i)$

$x_M \leftarrow a_L \text{ XOR } G(x_H, b_j)$

(where a high-order block of the storage content of the state storage section is denoted by a_H, an intermediate-order block of the storage content of the state storage section by a_M, a low-order block of the storage content of the state storage section by a_L, an ith block of said buffer storage section by b_i, said nonlinear transformation section by F(a, b) and G(a, b), substitution of data by ←, a high-order block of a transformation result by x_H, and an intermediate-order block of the transformation result by x_M, a low-order block of the the transformation result by x_L, and it is assumed that $i \neq j$).

5. A pseudorandom number generating apparatus according to claim 1, wherein

said state transformation section conducts the following processing:

$x_L \leftarrow a_M$;

$x_M \leftarrow a_H$ XOR $F(a_M, b_i)$

$x_H \leftarrow a_L$ XOR $G(a_M, b_j)$

(where a high-order block of the storage content of the state storage section is denoted by a_H, an intermediate-order block of the storage content of the state storage section by a_M, a low-order block of the storage content of the state storage section by a_L, a jth block of said buffer storage section by bj, said nonlinear transformation section by F(a, b) and G(a, b), substitution of data by ←, a high-order block of a transformation result by x_H, and an intermediate-order block of the transformation result by x_M, a low-order block of the transformation result by x_L, and it is assumed that $i \neq j$).

6. A pseudorandom number generating apparatus according to claim 1, wherein

one block is formed of 64 bits, and

said nonlinear transformation section further comprises S-boxes for dividing an input block by taking 8 bits as the unit and conducting nonlinear transformation, and comprises a processing section for conducting the following processing:

```
p ← a XOR b,
ti ← S[pi] (1 ≦ i ≦ 8);
uH ← $t_1||t_2||t_3||t_4$;
uL ← $t_5||t_6||t_7||t_8$;
uX ← uX XOR SHR8(uX), X={L, H};
uX ← uX XOR SHL16(uX), X={L, H};
uL ← uH AND 0xf0f0f0f0;
uH ← uL AND 0x0f0f0f0f;
out ← uH || uL;
```

(where an input from the state storage section is denoted by "a", an input from the buffer by "b", substitution of data by ←, S-box outputs by t_1, t_2, t_3, t_4, t_5, t_6, t_7 and t_8 in the descending order, or S[x], and an x-bit right shift and an x-bit left shift in a 64-bit width respectively by SHR_x and SHL_x, and it is assumed that $p = p_1||p_2||p_3||p_4||p_5||p_6||p_7||p_8$ (1 ≦ i ≦ 8)).

7. A pseudorandom number generating apparatus according to claim 1, wherein

said buffer has a capacity of 32 blocks, and said buffer transformation section comprises a processing section for conducting the steps of:

outputting blocks included in 32 blocks output by said buffer except a 25th high-order block and a 32nd high-order block, as blocks lowered in order by one;

10046157 .041502

conducting an exclusive OR-ing operation on the 32nd block with its high-order bits and its low-order bits interchanged and the 25th block, and outputting a result of the operation as a 24th block; and

conducting an exclusive OR-ing operation on the 32nd block and one block output from the state storage section, and outputting a result of the operation as a 1st block.

8. A decryption apparatus comprising:

a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of plaintext data to be encrypted; and

an operation section for conducting an exclusive OR-ing operation on the generated pseudorandom number sequence and the plaintext data, thereby calculating ciphertext data and outputting the ciphertext data, and

said pseudorandom number generating apparatus comprises:

a state storage section;

a buffer;

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation;

a state storage control section for updating an internal state of said state storage section by

10096152.041602

using the output of said state transformation section according to a clock; and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs; and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

9. A decryption apparatus comprising:

a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of ciphertext data, by using information for determining a random number sequence used when generating the ciphertext data to be decrypted; and

an operation section for conducting exclusive OR-ing operation on the generated pseudorandom number sequence and the ciphertext data, and thereby calculating plaintext data, and outputting the plaintext data, and

said pseudorandom number generating apparatus

10045167.011502

comprises:

a state storage section;

a buffer;

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation;

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock; and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs; and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

10. A pseudorandom number generating program that implements, in a computer including a storage device and a processor:

a state storage section;

a buffer;

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation;

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock; and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

wherein

said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs; and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

11. A pseudorandom number generating apparatus according to claim 1, wherein

said state transformation section conducts the following processing:

$X_H \leftarrow A_M$

10045157.041502

$X_M \leftarrow A_L$ XOR $F(A_M, B_I)$

$X_L \leftarrow A_H$ XOR $G(A_M, B_J)$

(where a high-order block of the storage content of the state storage section is denoted by A_H, an intermediate-order block of the storage content of the state storage section by A_M, a low-order block of the storage content of the state storage section by A_L, an Ith block of said buffer storage section by B_I, said nonlinear transformation section by F(A, B) and G(A, B), data inputting by $\leftarrow$, a high-order block of a transformation result by X_H, and an intermediate-order block of the transformation result by X_M, a low-order block of the transformation result by X, and it is assumed that $I \neq J$).

12. A pseudorandom number generating apparatus according to claim 1, wherein

one block is formed of 64 bits, and

said nonlinear transformation section further comprises S-boxes for dividing an input block by taking 8 bits as the unit and conducting nonlinear transformation, an MDS matrix for conducting linear transformation on outputs of the S-boxes by taking 32 bits as unit, and a processing section for conducting the following processing:

$P \leftarrow A$ XOR B;

$T_I \leftarrow S[P_I]$ $(1 \leqq I \leqq 8)$;

$U_H \leftarrow MDS_1(T_1, T_2, T_3, T_4)$;

$U_L \leftarrow MDS_2(T_5, T_6, T_7, T_8)$;

$U_H = X_1 \,||\, X_2 \,||\, X_3 \,||\, X_4$

$U_L = X_5 \;||\; X_6 \;||\; X_7 \;||\; X_8$

$OUT \leftarrow X_5 \;||\; X_6 \;||\; X_3 \;||\; X_4 \;||\; X_1 \;||\; X_2 \;||\; X_7 \;||\; X_8$;

(where an input from the state storage section is denoted by "A", an input from the buffer storage section by "B", substitution of data by ←, S-box outputs by T_1, T_2, T_3, T_4, T_5, T_6, T_7 and T_8 in the descending order, or S[X], and a transformation section using the MDS matrix by $MDS(T_a, T_b, T_c, T_d)$, and it is assumed that $P = P_1||P_2||P_3||P_4||P_5||P_6||P_7||P_8$ $(1 \leqq I \leqq 8)$).

10045167.011502

13. A pseudorandom number generating apparatus according to claim 1, wherein

said buffer has a capacity of 18 blocks, and said buffer transformation section comprises a processing section for conducting the steps of:

outputting blocks included in 18 blocks output by said buffer except a 2nd high-order block, a 12th high-order block, and an 18th high-order block, as blocks lowered in order by one;

conducting an exclusive OR-ing operation on the 2nd block and a 7th block, and outputting a result of the operation as a 3rd block;

conducting an exclusive OR-ing operation on a 15th block with its high-order half block and its low-order half block interchanged and the 12th block, and outputting a result of the operation as a 13th block; and

conducting an exclusive OR-ing operation on the 18th block and one block output from the state storage section and outputting a result of the operation as a 1st block.

14. A pseudorandom number generating apparatus according to claim 1, wherein said pseudorandom number generating apparatus comprises:

a key transformation section for expanding key information to data having a size equivalent to the capacity of said buffer section, and inputting resultant data to said buffer section.

15. A pseudorandom number generating apparatus according to claim 1, wherein

said state storage section uses public parameters.

16. A pseudorandom number generating apparatus according to claim 1, wherein

one block is formed of 64 bits, and

said nonlinear transformation section further comprises S-boxes for dividing an input block by taking 8 bits as the unit and conducting nonlinear transformation, an MDS matrix for conducting linear transformation on outputs of the S-boxes by taking 32 bits as unit, and a processing section having a 64-bit constant for conducting the following processing:

```
$P \leftarrow A \text{ XOR } B;$
$T_I \leftarrow S[P_I] \ (1 \leqq I \leqq 8);$
$U_H \leftarrow MDS_1(T_1, T_2, T_3, T_4);$
$U_L \leftarrow MDS_2(T_5, T_6, T_7, T_8);$
```

$U_H = X_1 \ || \ X_2 \ || \ X_3 \ || \ X_4$;

$U_L = X_5 \ || \ X_6 \ || \ X_7 \ || \ X_8$;

$Z \leftarrow X_5 \ || \ X_6 \ || \ X_3 \ || \ X_4 \ || \ X_1 \ || \ X_2 \ || \ X_7 \ || \ X_8$;

OUT ← Z XOR C;

(where an input from the state storage section is denoted by "A", an input from the buffer storage section by "B", substitution of data by ←, S-box outputs by T_1, T_2, T_3, T_4, T_5, T_6, T_7 and T_8 in the descending order, or S[X], and a transformation section using the MDS matrix by MDS(T_a, T_b, T_c, T_d), the constant by C, and it is assumed that $P = P_1||P_2||P_3||P_4||P_5||P_6||P_7||P_8$ ($1 \leqq I \leqq 8$)).

17. A pseudorandom number generating apparatus according to claim 16, wherein

when said constant C is divided into 8-bit blocks, at least one block has a value different from values of other blocks.

18. A pseudorandom number generating apparatus according to claim 1, wherein

said buffer has a capacity of 16 blocks, and said buffer transformation section comprises a processing section for conducting the steps of:

outputting blocks included in 16 blocks output by said buffer except a 4th high-order block, a 10th high-order block, and a 16th high-order block, as blocks lowered in order by one;

conducting an exclusive OR-ing operation on the 4th block and an 8th block, and outputting a result

10046157 .041502

of the operation as a 5th block;

conducting an exclusive OR-ing operation on a 14th block with its high-order half block and its low-order half block interchanged and the 10th block, and outputting a result of the operation as an 11th block; and

conducting an exclusive OR-ing operation on the 16th block and one block output from the state storage section and outputting a result of the operation as a 1st block.

19. A pseudorandom number generating apparatus according to claim 1, wherein

said pseudorandom number generating apparatus comprises a key transformation section supplied with key information and a diversification parameter, and a control section for controlling said key transformation section, and

said key transformation control section

controls said key transformation section so as to expand said key information to data having a size equal to a capacity of said buffer section, input resultant data to said buffer section, expand said key information to data having a size equal to a capacity of said state section, and input resultant data to said state section, and controls said state transformation section and said key transformation section so as to further update data of said state section, by using said key information expanded and input to said state

10016157.011502

section, and said diversification parameter.

10061567.071502